Configuration des commutateurs IP Cisco

ONTAP MetroCluster

NetApp
February 13, 2026

Sommaire

Configuration des commutateurs IP Cisco

Configurer les commutateurs IP Cisco pour l'interconnexion des clusters et la connectivité IP MetroCluster backend

Vous devez configurer les switchs IP Cisco pour une utilisation en tant qu'interconnexion de cluster et pour la connectivité IP MetroCluster back-end.

Description de la tâche

Plusieurs procédures de cette section sont des procédures indépendantes et vous n'avez qu'à exécuter celles que vous êtes dirigé vers ou qui sont pertinentes pour votre tâche.

Réinitialisation des paramètres d'usine du commutateur IP Cisco

Avant d'installer un fichier RCF, vous devez effacer la configuration du commutateur Cisco et effectuer une configuration de base. Cette procédure est obligatoire lorsque vous souhaitez réinstaller le même fichier RCF après l'échec d'une installation précédente ou si vous souhaitez installer une nouvelle version d'un fichier RCF.

Description de la tâche

- Vous devez répéter ces étapes sur chacun des commutateurs IP de la configuration MetroCluster IP.
- Vous devez être connecté au commutateur à l'aide de la console série.
- Cette tâche réinitialise la configuration du réseau de gestion.

Étapes

1. Rétablir les paramètres d'usine du commutateur :

   a. Effacez la configuration existante :

      ```
      write erase
      ```

   b. Recharger le logiciel du contacteur :

      ```
      reload
      ```

      Le système redémarre et entre dans l'assistant de configuration. Au cours du démarrage, si vous recevez l'invite « abandonner la mise en service automatique et poursuivre la configuration normale ? (oui/non)", you should respond `yes pour continuer.

   c. Dans l'assistant de configuration, entrez les paramètres de base du commutateur :

      - Mot de passe d'administrateur
      - Nom du commutateur
      - Configuration de gestion hors bande
      - Passerelle par défaut
      - Service SSH (RSA)

        Une fois l'assistant de configuration terminé, le commutateur redémarre.

d. Lorsque vous y êtes invité, entrez le nom d'utilisateur et le mot de passe pour vous connecter au commutateur.

L'exemple suivant montre les invites et les réponses système lors de la configuration du commutateur. Les supports d'angle (<<<) indique où vous saisissez les informations.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

    Enter the password for "admin": password
  Confirm the password for "admin": password
         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```

Vous entrez des informations de base dans les invites suivantes, notamment le nom du commutateur, l'adresse de gestion et la passerelle, et sélectionnez SSH avec RSA.

Cet exemple montre les informations minimales requises pour configurer la FCR. Des options supplémentaires peuvent être configurées une fois la FCR appliquée. Par exemple, vous pouvez configurer SNMPv3, NTP ou SCP/SFTP après avoir appliqué le RCF.

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
    Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
    Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

Le jeu d’invites final termine la configuration :

```
The following configuration will be applied:
  password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
  no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Enregistrez la configuration :

```
IP_switch-A-1# copy running-config startup-config
```

3. Redémarrez le commutateur et attendez que le commutateur se recharge :

```
IP_switch-A-1# reload
```

4. Répétez les étapes précédentes sur les trois autres commutateurs de la configuration MetroCluster IP.

Téléchargement et installation du logiciel du commutateur Cisco NX-OS

Vous devez télécharger le fichier du système d'exploitation du switch et le fichier RCF sur chaque commutateur de la configuration IP de MetroCluster.

Description de la tâche

Cette tâche nécessite un logiciel de transfert de fichiers, tel que FTP, TFTP, SFTP ou SCP, pour copier les fichiers sur les commutateurs.

Ces étapes doivent être répétées sur chacun des commutateurs IP de la configuration MetroCluster IP.

Vous devez utiliser la version du logiciel de commutation prise en charge.

"NetApp Hardware Universe"

Étapes

1. Téléchargez le fichier logiciel NX-OS pris en charge.

   "Téléchargement de logiciels Cisco"

2. Copier le logiciel du commutateur sur le commutateur :

   ```
   copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf
   management
   ```

   Dans cet exemple, le fichier nxos.7.0.3.I4.6.bin et l'image EPLD sont copiés du serveur SFTP 10.10.99.99 vers le bootflash local :

```
IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
/bootflash/nxos.7.0.3.I4.6.bin
Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
/tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
01:32
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/n9000-
epld.9.3.5.img bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/n9000-epld.9.3.5.img  /bootflash/n9000-
epld.9.3.5.img
Fetching /tftpboot/n9000-epld.9.3.5.img to /bootflash/n9000-
epld.9.3.5.img
/tftpboot/n9000-epld.9.3.5.img                161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

3. Vérifiez sur chaque commutateur que les fichiers de commutateur NX-OS sont présents dans le répertoire bootflash de chaque commutateur :

   `dir bootflash:`

   L'exemple suivant montre que les fichiers sont présents sur IP_switch_A_1 :

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Installez le logiciel du commutateur :

   `install all nxos bootflash:nxos.version-number.bin`

   Le commutateur se recharge automatiquement (redémarre) après l'installation du logiciel du commutateur.

   L'exemple suivant montre l'installation du logiciel sur IP_switch_A_1 :

```
IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 100%
-- SUCCESS

Performing module support checks.            [####################] 100%
-- SUCCESS

Notifying services about system upgrade.     [####################] 100%
```

```
-- SUCCESS



Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not
hitless



Images will be upgraded according to following table:
Module       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     1        nxos               7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y


Install is in progress, please wait.

Performing runtime checks.         [####################] 100%    --
SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS


Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#
```

5. Attendre que le commutateur se recharge, puis se connecter au commutateur.

   Une fois le commutateur redémarré, l'invite de connexion s'affiche :

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Vérifier que le logiciel du commutateur a été installé :
   `show version`

   L'exemple suivant montre la sortie :

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Mettre à niveau l’image EPLD et redémarrer le commutateur.

```
IP_switch_A_1# install epld bootflash:n9000-epld.9.3.5.img module 1
Compatibility check:
Module        Type         Upgradable    Impact      Reason
------  ------------------ ------------ ----------- -----------------
     1         SUP         Yes           disruptive  Module Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type   EPLD              Running-Version   New-Version  Upg-
Required
------- ------ ----------------- ----------------- ------------
------------
     1  SUP    MI FPGA           0x07              0x07         No
     1  SUP    IO FPGA           0x17              0x19         Yes
     1  SUP    MI FPGA2          0x02              0x02         No
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (     64 of      64 sectors)
Module 1 EPLD upgrade is successful.
Module   Type  Upgrade-Result
-------- ----- --------------
     1   SUP   Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
```

8. après le redémarrage du commutateur, reconnectez-vous et vérifiez que la nouvelle version de EPLD a été chargée avec succès.

   ```
   show version module 1 epld
   ```

9. Répétez ces étapes sur les trois commutateurs IP restants de la configuration IP MetroCluster.

Téléchargement et installation des fichiers Cisco IP RCF

Vous devez générer et installer le fichier RCF sur chaque switch de configuration MetroCluster IP.

Description de la tâche

Cette tâche nécessite un logiciel de transfert de fichiers, tel que FTP, TFTP, SFTP ou SCP, pour copier les fichiers sur les commutateurs.

Ces étapes doivent être répétées sur chacun des commutateurs IP de la configuration MetroCluster IP.

Vous devez utiliser la version du logiciel de commutation prise en charge.

"NetApp Hardware Universe"

Si vous utilisez une carte QSFP-to-SFP+, vous devrez peut-être configurer le port ISL en mode de vitesse natif au lieu du mode de vitesse d'arrachage. Consultez la documentation du fournisseur du commutateur pour déterminer le mode de vitesse du port ISL.

Il existe quatre fichiers RCF, un par pour chacun des quatre commutateurs de la configuration MetroCluster IP. Vous devez utiliser les fichiers RCF appropriés pour le modèle de commutateur que vous utilisez.

Commutateur	Fichier RCF
IP_switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_Switch_A_2	NX3232_v1.80_Switch-A2.txt
IP_Switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_Switch_B_2	NX3232_v1.80_Switch-B2.txt

Étapes

1. Générez les fichiers RCF Cisco pour MetroCluster IP.
   a. Téléchargez le "RcfFileGenerator pour MetroCluster IP"
   b. Générez le fichier RCF pour votre configuration à l'aide de RcfFileGenerator pour MetroCluster IP.

   > Les modifications apportées aux fichiers RCF après le téléchargement ne sont pas prises en charge.

2. Copier les fichiers RCF sur les commutateurs :
   a. Copier les fichiers RCF sur le premier commutateur :

      ```
      copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF
      bootflash: vrf management
      ```

      Dans cet exemple, le fichier RCF NX3232_v1.80_Switch-A1.txt est copié du serveur SFTP à 10.10.99.99 vers le bootflash local. Vous devez utiliser l'adresse IP de votre serveur TFTP/SFTP et le nom du fichier RCF que vous devez installer.

```
IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/NX3232_v1.80_Switch-A1.txt bootflash:
vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141     5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#
```

a. Répétez la sous-étape précédente pour chacun des trois autres commutateurs en étant sûr de copier le fichier RCF correspondant sur le commutateur correspondant.

3. Vérifiez sur chaque commutateur que le fichier RCF est présent dans le répertoire bootflash de chaque commutateur :

   `dir bootflash:`

   L'exemple suivant montre que les fichiers sont présents sur IP_switch_A_1 :

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
5514    Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
                  .
                  .
                  .

Usage for bootflash://sup-local
1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Configurez les régions TCAM sur les switchs Cisco 3132Q-V et Cisco 3232C.

   Ignorez cette étape si vous ne disposez pas de switchs Cisco 3132Q-V ou Cisco 3232C.

   a. Sur le commutateur Cisco 3132Q-V, définissez les régions TCAM suivantes :

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

b. Sur le switch Cisco 3232C, définissez les régions TCAM suivantes :

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl-lite 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

c. Après avoir défini les régions du TCAM, enregistrez la configuration et rechargez le commutateur :

```
copy running-config startup-config
reload
```

5. Copiez le fichier RCF correspondant de la mémoire bootflash locale vers la configuration en cours d'exécution sur chaque commutateur :

   `copy bootflash:switch-specific-RCF.txt running-config`

6. Copiez les fichiers RCF de la configuration en cours d'exécution vers la configuration de démarrage de chaque commutateur :

   `copy running-config startup-config`

   Vous devez voir les résultats similaires à ce qui suit :

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch-A-1# copy running-config startup-config
```

7. Recharger l'interrupteur :

   `reload`

```
IP_switch_A_1# reload
```

8. Répétez les étapes précédentes sur les trois autres commutateurs de la configuration MetroCluster IP.

Définition de la correction d'erreurs de renvoi pour les systèmes utilisant une connectivité à 25 Gbit/s.

Si votre système est configuré avec une connectivité 25 Gbit/s, vous devez définir manuellement le paramètre fec (Forward Error correction) sur Off après avoir appliqué le fichier RCF. Le fichier RCF n'applique pas ce paramètre.

Description de la tâche

Les ports 25 Gbit/s doivent être câblés avant d'effectuer cette procédure.

"Affectation des ports de plateforme pour les switchs Cisco 3232C ou Cisco 9336C"

Cette tâche s'applique uniquement aux plates-formes utilisant une connectivité 25 Gbit/s :

- AFF A300
- FAS 8200
- FAS 500f
- AFF A250

Cette tâche doit être effectuée sur les quatre commutateurs de la configuration IP MetroCluster.

Étapes

1. Définissez le paramètre fec sur Off sur chaque port 25 Gbit/s connecté à un module de contrôleur, puis copiez la configuration en cours d'exécution sur la configuration de démarrage :

   a. Passer en mode configuration : `config t`

   b. Spécifiez l'interface 25 Gbit/s à configurer : `interface interface-ID`

   c. Réglez fec sur Arrêt : `fec off`

   d. Répétez les étapes précédentes pour chaque port 25 Gbit/s du commutateur.

   e. Quitter le mode de configuration : `exit`

   L'exemple suivant montre les commandes de l'interface Ethernet1/25/1 sur le commutateur IP_switch_A_1 :

```
IP_switch_A_1# conf t
IP_switch_A_1(config)# interface Ethernet1/25/1
IP_switch_A_1(config-if)# fec off
IP_switch_A_1(config-if)# exit
IP_switch_A_1(config-if)# end
IP_switch_A_1# copy running-config startup-config
```

2. Répétez l'étape précédente sur les trois autres commutateurs de la configuration MetroCluster IP.

Désactivez les ports ISL et les canaux de port inutilisés

NetApp recommande de désactiver les ports ISL et les canaux de port inutilisés afin d'éviter les alertes d'intégrité inutiles.

1. Identifier les ports ISL et les canaux de port inutilisés :

   ```
   show interface brief
   ```

2. Désactivez les ports ISL et les canaux de port inutilisés.

   Vous devez exécuter les commandes suivantes pour chaque port ou canal de port non utilisé identifié.

   ```
   SwitchA_1# config t
   Enter configuration commands, one per line. End with CNTL/Z.
   SwitchA_1(config)# int Eth1/14
   SwitchA_1(config-if)# shutdown
   SwitchA_12(config-if)# exit
   SwitchA_1(config-if)# copy running-config startup-config
   [########################################] 100%
   Copy complete, now saving to disk (please wait)...
   Copy complete.
   ```

Configurer le cryptage MACsec sur les commutateurs Cisco 9336C dans un site IP MetroCluster

Le cryptage MACsec ne peut être appliqué qu'aux ports WAN ISL.

Configurez le cryptage MACsec sur les commutateurs Cisco 9336C

Vous devez uniquement configurer le cryptage MACsec sur les ports WAN ISL qui s'exécutent entre les sites. Vous devez configurer MACsec après avoir appliqué le fichier RCF correct.

Conditions de licence pour MACsec

MACsec nécessite une licence de sécurité. Pour une explication complète du schéma de licence Cisco NX-OS et de la manière d'obtenir et de demander des licences, consultez le "Guide des licences Cisco NX-OS"

Activez les liens ISL de Cisco MACsec dans les configurations IP de MetroCluster

Vous pouvez activer le cryptage MACsec pour les commutateurs Cisco 9336C sur les liens ISL WAN dans une configuration IP MetroCluster.

Étapes

1. Passer en mode de configuration globale :

   ```
   configure terminal
   ```

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. Activer MACsec et MKA sur le périphérique :

   `feature macsec`

   ```
   IP_switch_A_1(config)# feature macsec
   ```

3. Copier la configuration en cours d'exécution dans la configuration de démarrage :

   `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

Configurer une chaîne de clé MACsec et des clés

Vous pouvez créer une chaîne de clés MACsec ou des clés sur votre configuration.

Key Lifetime et hitless Key Rollover

Un trousseau MACsec peut avoir plusieurs clés pré-partagées (PSK), chacune configurée avec un ID de clé et une durée de vie facultative. La durée de vie d'une clé indique à quel moment la clé s'active et expire. En l'absence d'une configuration à vie, la durée de vie par défaut est illimitée. Lorsqu'une durée de vie est configurée, MKA passe à la prochaine clé pré-partagée configurée dans le trousseau une fois la durée de vie écoulée. Le fuseau horaire de la clé peut être local ou UTC. Le fuseau horaire par défaut est UTC. Une clé peut se déployer sur une seconde clé dans le même trousseau si vous configurez la seconde clé (dans le trousseau) et configurez une durée de vie pour la première clé. Lorsque la durée de vie de la première clé expire, elle passe automatiquement à la clé suivante de la liste. Si la même clé est configurée sur les deux côtés de la liaison en même temps, le basculement de la clé est sans arrêt (c'est-à-dire, la clé se replace sans interruption de la circulation).

Étapes

1. Passer en mode de configuration globale :

   `configure terminal`

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. Pour masquer la chaîne d'octet de clé cryptée, remplacez la chaîne par un caractère générique dans la sortie du `show running-config` et `show startup-config` commandes :

   ```
   IP_switch_A_1(config)# key-chain macsec-psk no-show
   ```

   > ⓘ La chaîne octet est également masquée lorsque vous enregistrez la configuration dans un fichier.

   Par défaut, les clés PSK sont affichées au format crypté et peuvent être déchiffrées facilement. Cette

commande ne s'applique qu'aux chaînes de clés MACsec.

3. Créer une chaîne de clés MACsec pour contenir un jeu de clés MACsec et entrer le mode de configuration de la chaîne de clés MACsec :

   `key chain name macsec`

   ```
   IP_switch_A_1(config)# key chain 1 macsec
   IP_switch_A_1(config-macseckeychain)#
   ```

4. Créer une clé MACsec et entrer le mode de configuration de la clé MACsec :

   `key key-id`

   La plage est comprise entre 1 et 32 caractères hexadécimaux, et la taille maximale est de 64 caractères.

   ```
   IP_switch_A_1 switch(config-macseckeychain)# key 1000
   IP_switch_A_1 (config-macseckeychain-macseckey)#
   ```

5. Configurez la chaîne d'octet pour la clé :

   `key-octet-string octet-string cryptographic-algorithm AES_128_CMAC | AES_256_CMAC`

   ```
   IP_switch_A_1(config-macseckeychain-macseckey)# key-octet-string
   abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789
   cryptographic-algorithm AES_256_CMAC
   ```

   L'argument octet-chaîne peut contenir jusqu'à 64 caractères hexadécimaux. La clé octet est codée en interne, de sorte que la clé en texte clair n'apparaît pas dans la sortie du `show running-config macsec` commande.

6. Configurer une durée de vie d'envoi pour la clé (en secondes) :

   `send-lifetime start-time duration duration`

   ```
   IP_switch_A_1(config-macseckeychain-macseckey)# send-lifetime 00:00:00
   Oct 04 2020 duration 100000
   ```

   Par défaut, l'appareil traite l'heure de début comme UTC. L'argument heure de début correspond à l'heure et à la date auxquelles la clé devient active. L'argument de durée est la durée de vie en secondes. La longueur maximale est de 2147483646 secondes (environ 68 ans).

7. Copier la configuration en cours d'exécution dans la configuration de démarrage :

   `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

8. Affiche la configuration du trousseau :

   `show key chain name`

```
IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
```

Configurez une stratégie MACsec

Étapes

1. Passer en mode de configuration globale :

   `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Créer une stratégie MACsec :

   `macsec policy name`

```
IP_switch_A_1(config)# macsec policy abc
IP_switch_A_1(config-macsec-policy)#
```

3. Configurez l'un des chiffrements suivants : GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 ou GCM-AES-XPN-256 :

   `cipher-suite name`

```
IP_switch_A_1(config-macsec-policy)# cipher-suite GCM-AES-256
```

4. Configurez la priorité du serveur de clés pour rompre le lien entre les pairs lors d'un échange de clés :

   `key-server-priority number`

```
switch(config-macsec-policy)# key-server-priority 0
```

5. Configurez la stratégie de sécurité pour définir le traitement des données et des paquets de contrôle :

   `security-policy security policy`

Choisissez une stratégie de sécurité parmi les options suivantes :

- Doit-Secure — les paquets qui ne portent pas les en-têtes MACsec sont supprimés
- Devrait-Secure — les paquets qui ne portent pas d'en-têtes MACsec sont autorisés (il s'agit de la valeur par défaut)

```
IP_switch_A_1(config-macsec-policy)# security-policy should-secure
```

6. Configurez la fenêtre de protection de relecture de sorte que l'interface sécurisée n'accepte pas un paquet dont la taille de fenêtre configurée est inférieure à celle de la fenêtre : `window-size number`

   La taille de la fenêtre de protection de relecture représente le nombre maximum de trames hors séquence que MACsec accepte et ne sont pas supprimées. La plage va de 0 à 596000000.

   ```
   IP_switch_A_1(config-macsec-policy)# window-size 512
   ```

7. Configurer le temps en secondes pour forcer une nouvelle touche SAK :

   `sak-expiry-time time`

   Vous pouvez utiliser cette commande pour remplacer la clé de session par un intervalle de temps prévisible. La valeur par défaut est 0.

   ```
   IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
   ```

8. Configurez l'un des décalages de confidentialité suivants dans la trame de couche 2 où le chiffrement commence :

   `conf-offsetconfidentiality offset`

   Choisissez parmi les options suivantes :

   - CONF-OFFSET-0.
   - CONF-OFFSET-30.
   - CONF-OFFSET-50.

   ```
   IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
   ```

   Cette commande peut être nécessaire pour que les commutateurs intermédiaires utilisent des en-têtes de paquets (dmac, smac, etype) comme des balises MPLS.

9. Copier la configuration en cours d'exécution dans la configuration de démarrage :

   `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

10. Afficher la configuration de la stratégie MACsec :

    `show macsec policy`

```
IP_switch_A_1(config-macsec-policy)# show macsec policy
```

Activez le cryptage Cisco MACsec sur les interfaces

1. Passer en mode de configuration globale :

   `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Sélectionnez l'interface que vous avez configurée avec le cryptage MACsec.

   Vous pouvez spécifier le type et l'identité de l'interface. Pour un port Ethernet, utilisez le logement/port ethernet.

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

3. Ajoutez le trousseau et la stratégie à configurer sur l'interface pour ajouter la configuration MACsec :

   `macsec keychain keychain-name policy policy-name`

```
IP_switch_A_1(config-if)# macsec keychain 1 policy abc
```

4. Répétez les étapes 1 et 2 sur toutes les interfaces où le cryptage MACsec doit être configuré.
5. Copier la configuration en cours d'exécution dans la configuration de démarrage :

   `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Désactivez les liens ISL de Cisco MACsec dans les configurations IP de MetroCluster

Vous devrez peut-être désactiver le cryptage MACsec pour les commutateurs Cisco 9336C sur les liens ISL du réseau étendu dans une configuration IP MetroCluster.

Étapes

1. Passer en mode de configuration globale :

   `configure terminal`

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. Désactivez la configuration MACsec sur le périphérique :

   `macsec shutdown`

   ```
   IP_switch_A_1(config)# macsec shutdown
   ```

   La sélection de l'option « non » restaure la fonction MACsec.

3. Sélectionnez l'interface que vous avez déjà configurée avec MACsec.

   Vous pouvez spécifier le type et l'identité de l'interface. Pour un port Ethernet, utilisez le logement/port ethernet.

   ```
   IP_switch_A_1(config)# interface ethernet 1/15
   switch(config-if)#
   ```

4. Supprimez le trousseau et la stratégie configurés sur l'interface pour supprimer la configuration MACsec :

   `no macsec keychain keychain-name policy policy-name`

   ```
   IP_switch_A_1(config-if)# no macsec keychain 1 policy abc
   ```

5. Répétez les étapes 3 et 4 sur toutes les interfaces où MACsec est configuré.
6. Copier la configuration en cours d'exécution dans la configuration de démarrage :

   `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

Vérification de la configuration MACsec

Étapes

1. Répétez **tous** des procédures précédentes sur le deuxième commutateur de la configuration pour établir une session MACsec.

2. Exécutez les commandes suivantes pour vérifier que les deux commutateurs sont chiffrés :

   a. Exécuter : `show macsec mka summary`

   b. Exécuter : `show macsec mka session`

   c. Exécuter : `show macsec mka statistics`

   Vous pouvez vérifier la configuration MACsec à l'aide des commandes suivantes :

Commande	Affiche des informations sur…
`show macsec mka session interface typeslot/port number`	La session MKA de MACsec pour une interface spécifique ou pour toutes les interfaces
`show key chain name`	La configuration de la chaîne de clés
`show macsec mka summary`	La configuration MACsec MKA
`show macsec policy policy-name`	Configuration d'une stratégie MACsec spécifique ou de toutes les politiques MACsec

Informations sur le copyright

Informations sur les marques commerciales